**UNITED STATES DISTRICT COURT**
**WESTERN DISTRICT OF WASHINGTON**
**SEATTLE DIVISION**

| | |
|---|---|
| JOHN DOE, on behalf of his minor child, JACK DOE, and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>FRED HUTCHINSON CANCER CENTER, UNIVERSITY OF WASHINGTON SCHOOL OF MEDICINE, UW MEDICAL CENTER, HARBORVIEW MEDICAL CENTER, VALLEY MEDICAL CENTER, UW PHYSICIANS, UW NEIGHBORHOOD CLINICS (d/b/a UW MEDICINE PRIMARY CARE), AIRLIFT NORTHWEST, and CHILDREN'S UNIVERSITY MEDICAL GROUP,<br><br>Defendants. | No.<br><br>**CLASS ACTION COMPLAINT**<br><br>**DEMAND FOR JURY TRIAL** |

Plaintiff, John Doe, on behalf of his minor child, Jack Doe (hereinafter, "Plaintiff"), and on behalf of all others similarly situated, brings this Class Action Complaint against Defendants Fred Hutchinson Cancer Center d/b/a Fred Hutch ("Fred Hutch"), University of Washington School of Medicine, UW Medical Center, Harborview Medical Center, Valley Medical Center,



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

UW Physicians, UW Neighborhood Clinics (d/b/a UW Medicine Primary Care), Airlift Northwest, and Children's University Medical Group (together "Defendants" or "UW Medicine"), and their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to his own actions, counsel's investigations, and facts of public record.

## NATURE OF ACTION

1. This class action arises from Defendants' failure to protect highly sensitive data—which has resulted in a flood of extortionary threats by cybercriminals to Defendants' current and former patients.

2. "UW Medicine" is an integrated health system—comprising, *inter alia*, the named Defendants.[1]

3. Most relevant is Defendant Fred Hutchinson Cancer Center, which is a Washington nonprofit organization that focuses on cancer care and research.[2]

4. As such, Defendants store a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about their current and former patients. But Defendants lost control over that data when cybercriminals infiltrated their insufficiently protected computer systems in a data breach (the "Data Breach").

5. It is unknown for precisely how long the cybercriminals had access to Defendants' network before the breach was discovered. In other words, Defendants had no effective means to prevent, detect, stop, or mitigate breaches of their systems—thereby allowing cybercriminals unrestricted access to current and former patients' PII/PHI.

6. On information and belief, cybercriminals were able to breach Defendants' systems because Defendants failed to adequately train their employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI. In short,

---

[1] *UW Medicine Overview*, UNIVERSITY OF WASHINGTON, https://depts.washington.edu/uwmmktg/wp-content/uploads/2022/11/UWMedicine-Overview.pdf (last visited Dec. 9, 2023).

[2] *About Us*, FRED HUTCH, https://www.fredhutch.org/en/about.html (last visited Dec. 9, 2023).



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

Defendants' failures placed the Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

7. Worryingly, this isn't Defendants first data breach. After all, Defendants were *also* hacked on March 25, 2022.[3] The next day, Defendants "discovered suspicious activity associated with a single employee's business email account."[4]And Defendant admitted that during that 2022 data breach, "an unauthorized individual accessed the account."[5]

8. Thus, this most recent Data Breach—which gives rise to the claims discussed herein—is simply part and parcel of Defendants' pattern of negligently inadequate data security.

9. Jack Doe is a Data Breach victim, having received an email from UW Medicine notifying him that Fred Hutchinson Cancer Center had experienced a data breach and informing him that ransom demands were being made directly to breach victims, described in Exhibit A by Defendant Fred Hutchinson Cancer Center. Jack Doe received two such ransom demands informing him that his information was affected in the breach. Plaintiff John Doe brings this class action on behalf of himself, Jack Doe, and all others harmed by Defendants' misconduct.

10. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, current and former patients' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

## PARTIES

11. Plaintiff, John Doe, is natural person and citizen of Washington. He resides in Bainbridge Island, Washington, where he intends to remain. He is the parent of his minor child, Jack Doe.

12. Jack Doe, is a natural person and citizen of Washington. He resides in Bainbridge Island, Washington, where he intends to remain.

---

[3] *Notice of Data Breach*, CALIFORNIA ATTY GEN, https://oag.ca.gov/system/files/%28AD%20CM%2012M%29%20ELN-15938%20Fred%20Hutchinson%20CC.pdf (last visited Dec. 9, 2023).
[4] *Id.*
[5] *Id.*



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

13. Defendant, Fred Hutchinson Cancer Center, is a Washington Nonprofit Corporation with its principal place of business at 1100 Fairview Ave N, Seattle, Washington 98109.

14. Defendant, University of Washington School of Medicine, is a school of the University of Washington. Its principal place of business is at 1959 NE Pacific St, Seattle, Washington 98195.

15. Defendant, UW Medical Center, is an acute care hospital with two campuses—one at 1550 N 115th St, Seattle, Washington 98133, and the other at 1959 N.E. Pacific St., Seattle, Washington 98195.

16. Defendant, Harborview Medical Center, is an acute care hospital owned by King County and managed by UW Medicine under a long-term Hospital Services Agreement. Its principal place of business is at 325 Ninth Ave., Seattle, Washington 98104.

17. Defendant, Valley Medical Center, is a public acute care public hospital district operated pursuant to a Strategic Alliance Agreement with UW Medicine. Its principal place of business is at 400 S 43rd St, Renton, Washington 98055.

18. Defendant, UW Physicians, is an adult practice group of physicians and healthcare professionals. The University of Washington is its sole corporate member. Its principal place of business is at 701 5th Ave #700, Seattle, Washington 98104.

19. Defendant, UW Neighborhood Clinics d/b/a UW Medicine Primary Care, is a network of community-based primary and urgent care clinics. The University of Washington is its sole corporate member, with its principal place of business at 1410 NE Campus Pkwy, Seattle, Washington 98195.

20. Defendant, Airlift Northwest, is an air transport service owned by the University of Washington. Its principal place of business is at 6505 Perimeter Road South, Suite 200, Seattle, Washington 98108.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

21. Defendant Children's University Medical Group is non-profit group practice. One of its corporate members in the University of Washington. Its principal place of business is at 4800 Sand Point Way NE, Seattle, Washington 98105.

## JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Members of the proposed Class are citizens of different states than Defendant. And there are over 100 putative Class members.

23. This Court has personal jurisdiction over Defendants because they are headquartered in Washington, regularly conduct business in Washington, and have sufficient minimum contacts in Washington.

24. Venue is proper in this Court because Defendants' principal offices are in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

## BACKGROUND

***Defendants Collected and Stored the PII/PHI of Jack Doe and the Class***

25. Defendants comprise UW Medicine which is an integrated health system—including, *inter alia*, Fred Hutchinson Cancer Center which is a Washington nonprofit organization that focuses on cancer care and research.[6]

26. As part of their business, Defendants receive and maintain the PII/PHI of thousands of their current and former patients.

27. In collecting and maintaining the PII/PHI, Defendants agreed they would safeguard the data in accordance with their internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their PII/PHI.

[6] *About Us*, FRED HUTCH, https://www.fredhutch.org/en/about.html (last visited Dec. 9, 2023).



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

28. Under state and federal law, entities like Defendants have duties to protect their current and former patients' PII/PHI and to notify them about breaches. And Defendants recognize these duties as detailed *infra*.

29. Via its "Privacy Policy and Terms of Use," Fred Hutch declares that:

a. Fred Hutch has a Privacy Policy that describes how we collect information from you or about you, why we collect this information, how we will use or disclose this information."[7]

b. "In addition, Fred Hutch's Privacy Policy sets forth our general policies on information security."[8]

30. And via its "Joint Notice of Privacy Practices," UW Medicine—including University of Washington School of Medicine, UW Medical Center, Harborview Medical Center, Valley Medical Center, UW Physicians, UW Neighborhood Clinics d/b/a UW Medicine Primary Care, and Airlift Northwest—declare that:

a. "We are required by law to maintain the privacy and security of your protected health information."[9]

b. "We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[10]

c. "We must follow the duties and privacy practices described in this notice and give you a copy of it."[11]

d. "We will not use or share your information other than as described here unless you tell us we can in writing."[12]

---

[7] *Privacy Policy and Terms of Use*, FRED HUTCH, https://www.fredhutch.org/en/util/terms-privacy.html (last visited Dec. 9, 2023).
[8] *Id*.
[9] *Joint Notice of Privacy Practices*, FRED HUTCH (Dec. 19, 2022) https://www.uwmedicine.org/sites/stevie/files/2023-01/A11499.MED_.M%20-%20Notice%20of%20Privacy%20Practice%20BROCHURE%2011.01.22_a11y.pdf.
[10] *Id*.
[11] *Id*.
[12] *Id*.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

e. "Special laws apply to certain kinds of health information. There are extra legal protections for health information about sexually transmitted diseases, drug and alcohol abuse treatment records, mental health records, and HIV/AIDS information. When required by law, we will not share this type of information without your written permission."[13]

31. Similarly, in its "Notice of Privacy Practices," Defendant Children's University Medical Group declares (via its corporate member Seattle Children's Hospital) that "We are required by law" to:

a. "Protect the privacy of your information." [14]

b. "Provide this notice about our privacy practices."[15]

c. "Follow the privacy practices described in this notice."[16]

d. "Notify you if your patient health information has been compromised."[17]

e. "This notice gives you information about the use and disclosure of your patient health information by these providers: . . . UW Medicine, which includes University of Washington Physicians and other University organizations."[18]

f. "Other than the uses and disclosures listed in this notice, we will not use or share your patient health information without your written authorization."[19]

---

[13] *Id.*
[14] *Notice of Privacy Practices*, SEATTLE CHILDREN'S (Jan. 10, 2018) https://www.seattlechildrens.org/globalassets/documents/for-patients-and-families/pfe/pi397.pdf.
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

***Defendants' Data Breach***

32. On November 19, 2923, Defendants "detected unauthorized activity on our clinical network."[20] And Defendants believe that "the criminal group responsible is outside the United States."[21]

33. Defendants claim that "the UW Medicine system was not impacted."[22] But upon information and belief—and as detailed *infra*—the Data Breach did indeed impact the broader UW Medicine system. After all Defendants stated that "UW Medicine clinicians also provide care to patients at Fred Hutch and some services are provided across multiple Fred Hutch and UW Medicine locations."[23]

34. Defendant admitted that Class members are "receiv[ing] threatening spam email."[24]

35. Specifically, Defendant has confirmed that "threat actors" are actively sending messages which "demand[] a ransom."[25]

36. Thus far, Defendants have refused to—or have been unable to—to explain to the Class what types of PII/PHI were exposed.[26]

37. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendants' custody and control. And upon information and belief, the putative class is over one hundred members—as it includes their current and former patients.

38. And yet, Defendants waited until December 2023 before they began notifying the Class.

---

[20] *Update on Data Security Incident*, FRED HUTCH (Dec. 7, 2023) https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html.
[21] *Id*.
[22] *Id*.
[23] *Id*.
[24] *Id*.
[25] *Id*.
[26] *See id*.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

39. Thus, Defendants kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

40. And when Defendants did notify Plaintiff and the Class of the Data Breach, Defendants acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class:

a. "remain vigilant to protect against potential fraud and/or identity theft;"

b. "review[] your account statements;"

c. "monitor[] credit reports closely;"

d. "report any fraudulent activity or any suspected incidents of identity theft to appropriate law enforcement authorities, including the police, as well as the Federal Trade Commission;"

e. "file a report with the FBI's Internet Crime Complaint Center at ic3.gov;"

f. "contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580."[27]

41. Defendants failed their duties when their inadequate security practices caused the Data Breach. In other words, Defendants' negligence is evidenced by their failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendants caused widespread injury and monetary damages.

42. Since the breach, Defendants has promised to be "updating and enhancing systems to prevent external parties from accessing information."[28] But this is too little too late. Simply put, these measures—which Defendants now recognizes as necessary—should have been implemented *before* the Data Breach.

43. On information and belief, Defendants failed to adequately train their employees on reasonable cybersecurity protocols or implement reasonable security measures.

---

[27] *Id.*
[28] *Id.*



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

44. Further, the Notice of Data Breach shows that Defendants cannot—or will not—determine the full scope of the Data Breach, as Defendants has been unable to determine precisely what information was stolen and when.

45. Defendants have done little to remedy the Data Breach. And it is unclear if Defendant has offered *anyone* basic credit monitoring and identity related services or even fully identified the scope of the Data Breach.[29]

46. Because of Defendants' Data Breach, the sensitive PII/PHI of Plaintiff (Jack Doe) and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff (Jack Doe) and Class members.

47. Worryingly, Class members have begun to receive "threatening emails claiming names, Social Security numbers, medical history and other data of more than 800,000 patients had been compromised."[30]

48. The cybercriminals have then "demanded $50 to have the information [of the Class] scrubbed from the dark web."[31]

49. Specifically, one patient reported that "I got an email saying that 800,000 patient records had been leaked and mine was among them. If I didn't pay $50, they would start selling them on the dark web."[32]

---

[29] *See Update on Data Security Incident*, FRED HUTCH (Dec. 7, 2023) https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html.

[30] *Some Seattle cancer center patients are receiving threatening emails after last month's data breach*, ABC NEWS (Dec. 9, 2023) https://abcnews.go.com/Health/wireStory/seattle-cancer-center-patients-receiving-threatening-emails-after-105522808.

[31] Ayanna Amadi, *Seattle-Based Cancer Center Patients Face Data Breach Threats: A Deep Dive Into the Incident and Its Implications*, MEDRIVA (Dec. 9, 2023) https://medriva.com/breaking-news/seattle-based-cancer-center-patients-face-data-breach-threats-a-deep-dive-into-the-incident-and-its-implications/.

[32] *'DO NOT PAY IT': Fred Hutch warns of 'threatening spam emails' after cyberattack*, KING 5 (Dec. 7, 2023) https://www.king5.com/article/news/local/fred-hutch-warn-patients-threatening-emails-cyberattack/281-40365cfa-61c9-4395-91ad-2c819695d4c0.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

50. And thus far, at least *three hundred* (300) of Defendants' current and former patients have reported receiving similar emails.[33]

***Plaintiff's Experiences and Injuries***

51. Plaintiff John Doe is the parent and guardian of Jack Doe.

52. Jack Doe is a former patient of Defendants. He has no relationship with the Fred Hutchinson Cancer Center.

53. The only relationship Jack Doe has had with Defendants was being born at Northwest Hospital—now the "Northwest" campus of Defendant UW Medical Center. And when Jack Doe was approximately two weeks old, he had one follow up visit at the UW Medicine Northgate Clinic at 314 NE Thornton Pl., Seattle, Washington 98125.Thus, Defendants obtained and maintained Jack Doe's PII/PHI.

54. As a result, Jack Doe was injured by Defendants' Data Breach.

55. As a condition of receiving medical services, Jack Doe (via his parent and guardian John Doe) provided his PII/PHI to Defendants. Defendants used that PII/PHI to facilitate their provision of medical services and to collect payment.

56. Plaintiff provided his PII/PHI to Defendants and trusted they would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

57. Plaintiff reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of PII/PHI.

58. Plaintiff does not recall ever learning that his minor child, Jack Doe's, information was compromised in a data breach incident—other than the breach at issue here.

59. Plaintiff received an email from UW Medicine informing him that Defendant Fred Hutchinson Cancer Center had experienced a data breach and informing him that ransom demands

[33] Kate Walters, *Hundreds of patients receive threatening emails after Fred Hutch cyberattack*, KUOW (Dec. 6, 2023) https://www.kuow.org/stories/hundreds-of-patients-receive-threatening-emails-after-fred-hutch-cyberattack.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

were being made directly to breach victims by the cybercriminals that perpetrated the attack. As noted above, Plaintiff has no relationship with Defendant Fred Hutchinson Cancer Center, having never received medical services there, but is a former patient of the UW Medicine system.

60. Thus, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

61. Worryingly, Plaintiff has *already* received two of the extortionary message detailed *supra*. This message demanded the Plaintiff pay the ransom of $50 to have his highly sensitive information protected.

62. The risk to Plaintiff's child, Jack Doe, as a minor, is substantial given the minor's lack of established credit because his information can be used to create a "clean identity slate."

63. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts and researching the data breach to protect himself from identity theft.

64. Plaintiff John Doe, on behalf of his minor child Jack Doe, fears for Plaintiff Jack Doe's future personal financial security and worries about what information was exposed in the Data Breach.

65. Because of Defendants' Data Breach, Plaintiff John Doe has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

66. Plaintiff John Doe, on behalf of Plaintiff Jack Doe, suffered actual injury from the exposure and theft of his PII/PHI—which violates his rights to privacy.

67. Plaintiff John Doe, on behalf of Plaintiff Jack Doe, suffered actual injury in the form of damages to and diminution in the value of his PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendants were required to adequately protect.

68. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff's PII/PHI right in the hands of criminals.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

69. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

70. Today, Plaintiff has a continuing interest in ensuring that his PII/PHI—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

***Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft***

71. Because of Defendants' failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Defendants' possession—and is thus as risk for futures breaches so long as Defendants fails to take appropriate measures to protect the PII/PHI.

72. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can be worth up to $1,000.00 depending on the type of information obtained.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

73. The value of Plaintiff and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

74. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII/PHI far and wide.

75. One way that criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

76. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

77. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

78. Defendants disclosed the PII/PHI of Plaintiff and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the PII/PHI of Plaintiff and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

79. Defendants' failure to promptly and properly notify Plaintiff and Class members of the Data Breach exacerbated Plaintiff and Class members' injury by depriving them of the



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

80. The risk to Plaintiff Jack Doe and other potential minor Class members is substantial given their age and lack of established credit because their information can be used to create a "clean identity slate." It is not surprising, then, that one report found that children are 51% more likely be victims of identity theft than adults.[34] Cybercriminals on the dark web have been caught selling Social Security numbers of infants for $300 per number to be used on fraudulent tax returns. [35]

***Defendants Knew—Or Should Have Known—of the Risk of a Data Breach***

81. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

82. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[36] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[37] Those 330 reported breaches exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[38]

83. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have

---

[34] Avery Wolfe, *How Data Breaches Affect Children*, Axion Cyber Sols. (Mar. 15, 2018) (last visited Dec. 9, 2023), https://axiomcyber.com/data-breach/how-data-breaches-affect-children/.
[35] *Id.*
[36] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.
[37] *Id.*
[38] *Id.*



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

lesser IT defenses and a high incentive to regain access to their data quickly."[39]

84. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[40]

85. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendants.

***Defendants Failed to Follow FTC Guidelines***

86. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

87. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[41] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

88. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

89. Furthermore, the FTC explains that companies must:

---

[39] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[40] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Sept. 11, 2023).

[41] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

90. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

91. In short, Defendants' failure to use reasonable and appropriate measures to protect against unauthorized access to their current and former patients' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

***Defendants Failed to Follow Industry Standards***

92. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendants. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

93. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

94. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

95. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendants opened the door to the criminals—thereby causing the Data Breach.

***Defendants Violated HIPAA***

96. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[42]

97. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI and PHI is properly maintained.[43]

98. The Data Breach itself resulted from a combination of inadequacies showing Defendants failed to comply with safeguards mandated by HIPAA. Defendants' security failures include, but are not limited to:

[42] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[43] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

a. failing to ensure the confidentiality and integrity of electronic PHI that they create, receive, maintain and transmit in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. failing to ensure compliance with HIPAA security standards by Defendants' workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

99. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

## CLASS ACTION ALLEGATIONS

100. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of Jack Doe and all members of the following class:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach discovered by Defendants in November 2023, including all those individuals who received notice of the breach.

101. Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any Defendants' officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

102. Plaintiff reserves the right to amend the class definition.

103. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

104. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendants' custody and control. After all, Defendants already identified some individuals and sent them data breach notices.

105. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least one hundred members.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

106. Typicality. Plaintiff's claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

107. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

108. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII/PHI;

b. if Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendants were negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendants breached contract promises to safeguard Plaintiff and the Class's PII/PHI;

e. if Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendants' Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

109. Superiority. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendants would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

## FIRST CAUSE OF ACTION
### Negligence
### (On Behalf of Plaintiff and the Class)

110. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

111. Plaintiff and the Class (or their third-party agents) entrusted their PII/PHI to Defendants on the premise and with the understanding that Defendants would safeguard their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their PII/PHI to unauthorized third parties.

112. Defendants owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendants' failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

113. Defendants have full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

114. Defendants owed these duties to Plaintiff and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

practices. After all, Defendants actively sought and obtained Plaintiff and Class members' PII/PHI.

115. Defendants owed—to Plaintiff and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in their care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their PII/PHI.

116. Thus, Defendants owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

117. Defendants also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI they was no longer required to retain under applicable regulations.

118. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII/PHI of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

119. Defendants' duty to use reasonable security measures arose because of the special relationship that existed between Defendants and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class (or their third-party agents) entrusted Defendants with their confidential PII/PHI, a necessary part of obtaining services from Defendants.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

120. Under the FTC Act, 15 U.S.C. § 45, Defendants had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff and Class members' PII/PHI.

121. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff and the Class members' sensitive PII/PHI.

122. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI Defendants had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

123. Similarly, under HIPAA, Defendants had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class members' PHI.

124. Defendants violated their duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendants' conduct was particularly unreasonable given the nature and amount of PHI that Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

125. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendants hold vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the PII/PHI —whether by malware or otherwise.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

126. PII/PHI is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiff and Class members' and the importance of exercising reasonable care in handling it.

127. Defendants improperly and inadequately safeguarded the PII/PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

128. Defendants breached these duties as evidenced by the Data Breach.

129. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' PII/PHI by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in their employ who were responsible for making that happen.

130. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII/PHI of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff and Class members' injury.

131. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class members' injuries-in-fact.

132. Defendants have admitted that the PII/PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

133. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

134. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

135. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

## SECOND CAUSE OF ACTION
### Breach of Implied Contract
### (On Behalf of Plaintiff and the Class)

136. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

137. Plaintiff and Class members (or their third-party agents) were required to provide their PII/PHI to Defendants as a condition of receiving medical services provided by Defendants. Plaintiff and Class members (or their third-party agents) provided their PII/PHI to Defendants or their third-party agents in exchange for Defendants' medical services.

138. Plaintiff and Class members (or their third-party agents) reasonably understood that a portion of the funds they paid Defendants would be used to pay for adequate cybersecurity measures.

139. Plaintiff and Class members (or their third-party agents) reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendants' duties under state and federal law and their internal policies.

140. Plaintiff and the Class members (or their third-party agents) accepted Defendants' offers by disclosing their PII/PHI to Defendants or their third-party agents in exchange for medical services.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

141. In turn, and through internal policies, Defendants agreed to protect and not disclose the PII/PHI to unauthorized persons.

142. In their Privacy Policies, Defendants represented that they had a legal duty to protect Plaintiff's and Class Member's PII/PHI.

143. Implicit in the parties' agreement was that Defendants would provide Plaintiff and Class members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

144. After all, Plaintiff and Class members (or their third-party agents) would not have entrusted their PII/PHI to Defendants in the absence of such an agreement with Defendants.

145. Plaintiff and the Class (or their third-party agents) fully performed their obligations under the implied contracts with Defendants.

146. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

147. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

148. Defendants materially breached the contracts it entered with Plaintiff and Class members (or their third-party agents) by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into their computer systems that compromised such information.

c. failing to comply with industry standards;



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendants created, received, maintained, and transmitted.

149. In these and other ways, Defendants violated their duty of good faith and fair dealing.

150. Defendants' material breaches were the direct and proximate cause of Plaintiff's and Class members' injuries (as detailed *supra*).

151. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

152. Plaintiff and Class members (or their third-party agents) performed as required under the relevant agreements, or such performance was waived by Defendants' conduct.

## THIRD CAUSE OF ACTION
**Breach of Fiduciary Duty**
**(On Behalf of Plaintiff and the Class)**

153. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

154. Given the relationship between Defendants and Plaintiff and Class members, where Defendants became guardian of Plaintiff's and Class members' PII/PHI, Defendants became a fiduciary by their undertaking and guardianship of the PII/PHI, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' PII/PHI; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and does store.

155. Defendants has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendants' relationship with them—especially to secure their PII/PHI.

156. Because of the highly sensitive nature of the PII/PHI, Plaintiff and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendants'



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

position, to retain their PII/PHI had they known the reality of Defendants' inadequate data security practices.

157. Defendants breached their fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII/PHI.

158. Defendants also breached their fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

159. As a direct and proximate result of Defendants' breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

## FOURTH CAUSE OF ACTION
**Invasion of Privacy**
**(On Behalf of Plaintiff and the Class)**

160. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

161. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

162. Defendants owed a duty to their current and former patients, including Plaintiff and the Class, to keep this information confidential.

163. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class members' PII/PHI is highly offensive to a reasonable person.

164. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

165. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

166. Defendants acted with a knowing state of mind when they permitted the Data Breach because they knew their information security practices were inadequate.

167. Defendants acted with a knowing state of mind when they failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

168. Acting with knowledge, Defendants had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

169. As a proximate result of Defendants' acts and omissions, the private and sensitive PII/PHI of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

170. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

171. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII/PHI are still maintained by Defendants with their inadequate cybersecurity system and policies.

172. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendants' inability to safeguard the PII/PHI of Plaintiff and the Class.

173. In addition to injunctive relief, Plaintiff, on behalf of himself, Jack Doe, and the other Class members, also seeks compensatory damages for Defendants' invasion of privacy,



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

**FIFTH CAUSE OF ACTION**
**Unjust Enrichment**
**(On Behalf of Plaintiff and the Class)**

174. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

175. This claim is pleaded in the alternative to the breach of implied contract claim.

176. Plaintiff and Class members (or their third-party agents) conferred a benefit upon Defendants. After all, Defendants benefitted from using their PII/PHI and payment to provide services and/or collect payment.

177. Defendants appreciated or had knowledge of the benefits it received from Plaintiff and Class members (or their third-party agents). And Defendants benefited from receiving Plaintiff's and Class members' PII/PHI and payment, as this was used to provide services and/or collect payment.

178. Plaintiff and Class members (or their third-party agents) reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendants' duties under state and federal law and their internal policies.

179. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII/PHI.

180. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

181. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff's and Class members' PII/PHI and payment because Defendants failed to adequately protect their PII/PHI.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

182. Plaintiff and Class members have no adequate remedy at law.

183. Defendants should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that they received because of their misconduct.

**SIXTH CAUSE OF ACTION**
**Violation of Washington Consumer Protection Act**
**RCW 19.86.010, *et seq*.**
**(On Behalf of Plaintiff and the Class)**

184. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

185. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

186. Each Defendant is a "person" as described in RWC 19.86.010(1).

187. Defendants engage in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

188. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendants' practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

189. Defendants' failure to safeguard the PII/PHI exposed in the Data Breach constitutes an unfair act that offends public policy.

190. Defendants' failure to safeguard the PII/PHI compromised in the Data Breach caused substantial injury to Plaintiff and Class Members. Defendants' failure is not outweighed by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable by consumers.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

191. Defendants' failure to safeguard the PII/PHI disclosed in the Data Breach, and their failure to provide timely and complete notice of that Data Breach to the victims, is unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

192. In the course of conducting their business, Defendants committed "unfair or deceptive acts or practices" by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI, and violating the common law alleged herein in the process. Plaintiff and Class Members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. As described above, Defendants' wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

193. Defendants also violated the CPA by failing to timely notify, and by concealing from Plaintiff and Class Members, information regarding the unauthorized release and disclosure of their PII/PHI. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII/PHI and identities.

194. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendants' wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

195. The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

196. Defendants' unfair or deceptive acts or practices occurred in their trade or business and have injured and are capable of injuring a substantial portion of the public. Defendants'



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

general course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

197. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the CPA, Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their PII/PHI; (5) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

198. Unless restrained and enjoined, Defendants will continue to engage in the wrongful conduct (detailed *supra*) and more data breaches will occur. Plaintiff, therefore, on behalf of themselves and the Class, seek restitution and an injunction prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to it.

199. Plaintiff, on behalf of himself, Jack Doe, and Class Members, also seek to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiff, on behalf of themselves and Class Members, request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained not to exceed $25,000.00 per Class Member.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

**SEVENTH CAUSE OF ACTION**
**Violation of Washington Data Breach Disclosure Law**
**RCW 19.255.005, *et seq*.**
**(On Behalf of Plaintiff and the Class)**

200. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

201. Under RCW § 19.255.010(2), "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

202. Upon information and belief, this statute applies to Defendants because Defendants does not own nor license the PII/PHI in question. Instead, the owners and/or licensees of the PII/PHI are Plaintiff and the Class.

203. Here, the Data Breach led to "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendants, leading to a "breach of the security of [Defendants'] systems," as defined by RCW § 19.255.010.

204. Defendants failed to disclose that the PII/PHI—of Plaintiffs and Class Members—that had been compromised "immediately" upon discovery, and thus unreasonably delayed informing Plaintiffs and the proposed Class about the Data Breach.

205. Thus, Defendants violated the Washington Data Breach Disclosure Law.

**EIGHTH CAUSE OF ACTION**
**Violation of Washington Uniform Health Care Information Act (UHCIA)**
**RCW 70.02.005, *et seq*.**
**(On Behalf of Plaintiff and the Class)**

206. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

207. UHCIA declares that:

a. "Health care information is personal and sensitive information that if improperly used or released may do significant harm to a patient's interests in privacy, health care, or other interests." § 70.02.005(1).



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

b. "In order to retain the full trust and confidence of patients, health care providers have an interest in assuring that health care information is not improperly disclosed and in having clear and certain rules for the disclosure of health care information." § 70.02.005(3).

c. "It is the public policy of this state that a patient's interest in the proper use and disclosure of the patient's health care information survives even when the information is held by persons other than health care providers." § 70.02.005(4).

208. Here, each Defendant is a "health care provider" because they are "licensed, certified, registered, or otherwise authorized by the law of this state to provide health care in the ordinary course of business or practice of a profession." § 70.02.010(19).

209. Under § 70.02.020, "a health care provider, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider may not disclose health care information about a patient to any other person without the patient's written authorization."

210. Here, Defendants violated UHCIA because Defendants—via their Data Breach—disclosed health care information to third parties without patient authorization.

211. Thus, Plaintiff seeks, *inter alia*, all civil remedies available under § 70.02.170 including actual damages, attorneys' fees, and reasonable expenses.

## NINTH CAUSE OF ACTION
**Declaratory Judgment**
**(On Behalf of Plaintiff and the Class)**

212. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

213. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

214. In the fallout of the Data Breach, an actual controversy has arisen about Defendants' various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendants' actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

215. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendants has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendants breached, and continues to breach, their duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendants' breaches of their duties caused—and continues to cause—injuries to Plaintiff and Class members.

216. The Court should also issue corresponding injunctive relief requiring Defendants to use adequate security consistent with industry standards to protect the data entrusted to it.

217. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendants experiences a second data breach.

218. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class members' injuries.

219. If an injunction is not issued, the resulting hardship to Plaintiff and Class members far exceeds the minimal hardship that Defendants could experience if an injunction is issued.

220. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class members, and the public at large.



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

## PRAYER FOR RELIEF

Plaintiff and Class members respectfully request judgment against Defendants and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

D. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

## DEMAND FOR JURY TRIAL



TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

Plaintiff demands a jury trial for all claims so triable.

Date: December 10, 2023

By: /s/ Samuel J. Strauss, WSBA #46971

Samuel J. Strauss, WSBA #46971
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703-3515
Telephone: (608) 237-1775
Facsimile: (608) 509 4423
sam@turkestrauss.com

*Attorneys for Plaintiff and Proposed Class*